Issue: March 3, 2003

Utah Department of Health
Data Stewardship Policy

I. Purpose of Policy:

A. Assure data are treated as an asset and utilized to the fullest extent;

B. Assure wide access to and use of data within the limits of existing statutes, rules, federal requirements, Department policies, and relevant ethical principals;

C. Assure coordinated collection of data and requests for data;

D. Provide guidance for data sharing practices;

E. Assure that data are managed to protect confidentiality;

F. Assure that the data are used in the proper context;

G. Establish roles and responsibilities associated with the implementation of this policy.

II. Background:

Data are essential to the mission and purpose of the Utah Department of Health (Department). Data collected by organizational units or individuals within the Department are collected under the authority of the Department. The stewardship and use of those data are ultimately the responsibility of the Department. All Department employees and contracted individuals working for an organizational unit within the Department must protect the confidentiality of the data and are subject to the Department Confidentiality Policy.

The missions and purposes of organizational units within the Department often complement each other and sharing data helps the Department to accomplish its overall mission. In order to help the programs meet their goals, the Department supports data sharing between its organizational units whenever that sharing supports legitimate public health purposes.

Organizational units and their data stewards are responsible to ensure the best and proper use of data under their stewardship. They should facilitate and promote the sharing of data as an asset to support legitimate public health purposes. Comprehensive data sharing agreements are generally needed when sharing data with parties outside the Department. For data sharing within the Department, written policies, protocols, and agreements are encouraged for tracking purposes and for clarifying appropriate uses of data.

Data stewards may limit access to data resources when necessary to exercise appropriate stewardship of those data (e.g., preventing inappropriate disclosure of confidential data). However, the exercise of data stewardship includes the support of internal data sharing and does not include arbitrarily restricting access to data resources.

III. Policy

A. Responsibilities:

1. **General Employee Responsibilities** - All individuals in the Department who use health data have general data stewardship responsibilities. The general data stewardship responsibilities include:

    a. Protecting the confidentiality of identifiable health data by disclosing individually identifiable information only as allowed by this policy, other Department policy, or state or federal law;

b. Treating the Department's health data as a Department-wide asset;

c. Using the Department Data Inventory published on DOHnet, the Department's Intranet, or using the Department's Analytic Network Coordinating Team (ANCT) to verify that needed data do not already exist before engaging in collecting data;

d. Using Department data resources within the limits set by statutes, rules, federal requirements, Department policies, and relevant ethical principles; and

e. Facilitating appropriate use and sharing of health data in support of the mission of the Department, within the limits set by statutes, rules, federal requirements, Department policies, and relevant ethical principles.

2. **Division Responsibilities** - Each Division/Office Director whose organizational units/programs collect or hold health data is responsible to:

a. Determine which of its data resources are significant sources of information for disease and risk factor surveillance, needs assessment, policy making, and program evaluation;

b. Assign a data steward for each significant data resource under their management;

c. Publish (in the Department's Data Inventory on DOHnet) their names and contact information along with their assigned data resource inventory;

d. Include data stewards' assignments and responsibilities in the performance plans for named individuals;

e. Advise the data stewards under their supervision when data stewards bring issues to their attention for resolution;

f. Seek to include data sharing provisions in all federal or private grants and contracts entered into on behalf of the Department;

g. Seek resolution within the Department's chain of command for issues related to data use and data sharing; and

h. Assure that Institutional Review Board (IRB) or ethics committee human subjects review are obtained where appropriate.

3. **Director of Center for Health Data Responsibilities** – To bring consistency in data stewardship performance, the Director of Center for Health Data will directly conduct regular audits to review data sharing requests and their resolution and provide guidance to the appropriate data stewards or delegate the audits to an individual or to the ANCT.

4. **IRB Responsibilities** – refer to the IRB Bylaws and Mission Statement.

5. **Data Steward Responsibilities** – In addition to the general responsibilities of data stewardship described under point 1 above, each data steward shall, for all data under stewardship:

a. Update and maintain the relevant portions of the Department's Data Inventory on DOHnet;

b. Facilitate access to the data to the extent allowed by statutes, rules, federal requirements, Department policies, and relevant ethical principles;

c. Create and maintain data access, security and management plans;

d. Establish access policies and procedures that assure appropriate protection of both individual confidentiality/privacy and of the public trust under which those data are collected;

e. Create and maintain an adequate record of data collection and management procedures and practices (data management log);

f. Create and maintain disaster recovery and business continuity plans;

g. Assure that data are modified only in appropriate ways;

h. Follow state and federal legal requirements regarding release of data;

i. Comply with the terms of applicable legal agreements and contracts;

j. Assure that data are accessed only by authorized individuals and for authorized purposes;

k. Comply with requirements for registration of data records with the state archivist and fulfilling functions of the records officer;

l. Implement data sharing agreements where appropriate;

m. Seek advice and direction from supervisor for unusual data use and data sharing situations;

n. Assure that IRB reviews occur for uses of data that constitute human subjects research and that ethical reviews are conducted, where warranted, for non-research uses of data.

IV. Procedures for Sharing Data Among Department Programs:

Data sharing among Department's organizational units and their programs and systems is both supported and encouraged. The data requester for both one-time and ongoing sharing of data shall negotiate with the appropriate data steward. The source data steward(s) shall document the data sharing decisions in an informal data sharing agreement, by tracking the:

A. Party, or parties, with whom data are shared;

B. Nature/type of the data shared;

C. Intended uses of the data;

D. Frequency of the exchange of data.

Formal data sharing agreements are not required but may be developed by the data stewards. Documented policies, procedures, and protocols that clarify appropriate uses of data are encouraged.

V. Procedures for Release of Identifiable Health Data to Parties Outside the Department for Research:

A. All requests for access to non-publicly available identifiable health data, made for research purposes by any outside organization or individual, shall be directed to the appropriate data steward. Requests must be in writing and must include:

1. Nature/type of the data requested;

2. Purposes for which the data will be used;

3. Allowable uses of the data;

4. Assurance that the confidentiality and security of the data will be maintained;

5. Provisions for data storage, retention, and disposal.

B. Before deciding to release individually identifiable health data, the data steward(s) shall consider the following prior to releasing the data:

1. **Need for the Requested Data** – Does there exist a compelling need or absolute necessity for the requested data; can the data be replaced with non-identifiable data; is this the minimum data to meet the need; does the need for this data justify the risk of disclosure; or can test data be used?

2. **Use of the Data** – Will the data be used for legitimate purposes; will data use be restricted to the stated purposes?

3. **Confidentiality/Security of the Data** – Will the data be safeguarded and protected; does there exist a potential for violation of the confidentiality of the data or actual physical theft or loss; will the data be disclosed or re-released to anyone at any time under any circumstances; and will the data be properly disposed?

C. If uncertain if release is allowable, the data stewards shall obtain advice and direction from their immediate supervisor who will take the issue up the chain of command. If the proposed uses of the data constitute human subjects research or if statutes, rules, federal requirements, and Department policies require it, the data steward shall assure that human subjects review and approval by an appropriate IRB is obtained.

D. Data sharing agreements are required for all external sharing of identifiable health data.

E. The data steward will evaluate the feasibility and difficulty to produce the data and may request that an appropriate charge be paid to recover costs and applicable fees.

VI. Procedures for Release of De-identified Health Data to Parties Outside the Department:

Requests for de-identified health data by any outside organization or individual must be directed to the appropriate data steward.

A. If the data are available publicly, the data steward shall direct the requestor to the appropriate source location.

B. If the data are not publicly or generally available, the data steward will evaluate the feasibility and difficulty to produce the de-identified data and may request that an appropriate charge be paid to recover costs and applicable fees.

VII. Data Sharing Agreements

A. Data sharing agreements shall be used with parties outside of the Department:

1. When sharing identifiable health data;

2. When sharing health data that has been de-identified by removing fewer than all of the data elements specified in the safe harbor provisions of the HIPAA privacy regulation.

B. Data sharing agreements are not required to share data that has been de-identified by removing all or more of the data elements specified in the safe harbor provisions of the HIPAA privacy regulation, unless those data still could meet the definition of identifiable data included at the end of this document.

C. Data sharing agreements may be required to share data among Department programs depending on the applicable statutes and regulations.

D. Upon agreement from the data steward, or from the appropriate level of management, approval to access the data can be granted, with the following assurances given by the data requestor and recorded in a formal data sharing agreement:

- Party, or parties with whom data will be shared;
- Time period of the agreement;
- Nature/type of the data requested;
- Intended uses of the data;
- Frequency of the exchange of data;

- Requirement that the requestor will protect completely the confidentiality of the data provided;
- Requirement that the requestor will not disclose or release the identifiable health data without specific written permission from the Department;
- Requirement that the requestor will report immediately the loss or theft of any identifiable data or related confidential materials to the appropriate Data Steward;
- How the requestor will maintain the confidentiality and the security of the data;
- A statement that the Department is either the owner or has rights to control the use and dissemination of the data;
- Provision describing and how the data will be disposed of at the conclusion of the agreement;
- Assurances that the requestor will obey all state and federal laws regarding the use of the data;
- Specification of rights for audit of data use practices;
- Provisions regarding secondary release of the data;
- A provision that the recipient will hold the Department harmless from all liability arising from the recipient's use or disclosure of the data; and
- Consequences of violation of the agreement.

E. A data sharing agreement sample is attached as an appendix. Data sharing agreements may change through time and may be modified to meet specific needs.

VIII. Unresolved Issues/Policy Implementation:

Any issues remaining unresolved upon implementation of this policy or questions regarding implementation or interpretation are to be brought to the attention of the Director, Center for Health Data.

IX. Appendix:

A. Definitions:

Several terms are explained for the purpose of creating a common understanding of the issues covered by this policy.

1. **Data stewardship**– The responsibility carried out on behalf of a larger group, institution, or the public in general to safeguard, protect, and optimize the use of the data resources. Data stewardship in the Utah Department of Health relates to the data collected by an organizational unit under the authority of the Department. Protecting the Department's data resources includes, and is subject to, all the statutes and rules that pertain to the data. A data steward does not have the right to conceal or hold protected health data for personal benefit, disclose protected health data without proper authorization, or arbitrarily limit access to the data.

2. **Health data** – Any data relating to the health status of people, living or dead; all forms of data relating to health including data on the extent and nature of the illness, disability and other aspects of well being; environmental, social and other health hazards; determinants of health.

3. **Identifiable health data** – [Title 26-3-1 Definition] "Identifiable health data" means any item, collection, or grouping of health data which makes the individual supplying it or described in it identifiable.

   With regard to individuals, the term means any item, collection or grouping of data which contains the name of the individual or any identifying number, symbol, other identifying characteristics, or any unique grouping of data, which, when combined with other available data, makes the individual recognizable. With regard to organizations that have received an assurance of non-disclosure from the Department, the term means, any item, collection or grouping of data, which makes the organization as recognizable as if a name had been affixed. Identifiable health data encompasses health data that identifies individuals by name, unique identifier, or other identifying characteristics. The definition also encompasses health data identifying organizations that have received an assurance of non-disclosure by the Department.

4. **Disclosure** – [Title 26-3-1 Definition] "Disclosure" or "disclose" means the communication of health data to any individual or organization outside the department.

5. **Institutional Review Board (IRB) –** An official Department body whose mission is to review for approval research projects involving human subjects. Certain statutes and rules define bona fide research approved by an IRB as one criterion for release of identifiable health data. Thus, IRB review and approval is required for certain uses of health data.

B. Data Sharing Agreement - Sample